REMARKS

The Examiner's action mailed on February 23, 2005 has been received and its contents carefully considered.

Claims 1-16 are pending in this application. Claim 1 is amended herein. Claim 1 remains the sole independent claim.

In the Action, claims 1-16 are rejected under 35 U.S.C. §103(e) as being obvious over Numao et al. (U.S. Patent No. 6,647,388) in view of Schneider et al. (U.S. Patent No. 6,105,027). Claim 1 is amended herein to more clearly distinguish the present invention over the applied prior art references.

Regarding claim 1, the Examiner points in the Action to Numao as disclosing a document management system for limiting user access to a registered document, comprising: a first storage means for registering a document to be accessed (figure 1, column 8, lines 10-28, column 16, lines 50-54); and a second storage means for registering access controlling information including a specific character string and identification data (figure 1, column 8 lines 10-28, column 16 lines 50-54). However, the Examiner acknowledges that Numao does not clearly teach that the controlling information includes a specific character string and identification data. To address this deficiency in Numao, the Examiner points to Schneider as disclosing an access control system using a plurality of filters, each filter having a local copy of access control information (column 6, lines 24-26). The Examiner argues that in the Schneider system, the database contains a data sensitive level for each information resource (column 18, lines 5-12), and further that as shown in figure 6, column 603 corresponds to the "identification data" recited in the present application, and the requirement in columns 607-609 corresponds to the "specific character string" of the present application. The Examiner cites Schneider column 19, lines 10-20, as teaching the limitation in the claim 1, "access to said document is limited in accordance with contents of said access controlling information, when the access to said document is thereafter requested, if said document contains added identification data". The Examiner argues that it would have been obvious to one of ordinary skill in the art at the time

the invention was made to apply the teaching of Schneider to the invention of Numao because the combination would increase the security of a document by limiting access to the document using identification data and the specific character string.

The Applicants disagree in several respects with the Examiner's arguments regarding claim 1. First, as noted above, the Examiner asserts a correspondence between the "specific character string" recited in claim 1 and the requirement in columns 607-609 in figure 6 of Schneider. However, what Schneider discloses is that Figure 6 is a table used by the access filters 203 for defining the relationship between sensitivity and trust levels and authentication and encryption techniques (column 6, lines 55-57). The techniques employed in the access filters 203 to determine the minimum amount of security for a communication session are collectively termed SEND (Secure Encrypted Network Delivery). In SEND, access control database 301 (Schneider figure 3) contains a data sensitivity level for each information resource. The data sensitivity level indicates the level of secrecy associated with the information resource and is assigned to the information resource by the security administrator responsible for the resource (column 18, lines 3-12). In figure 6 of Schneider, the "minimum encryption" requirement in column 609 indicates how to encrypt data to which access is required and to have it accessed. In the first row of figure 6, for example, 3DES is the name of the encryption algorithm associated with the top secret sensitivity level. The "minimum authentication" requirement in column 607 indicates how to authenticate the user requesting access to an information resource. For example, a user who wishes to get access to resource with the sensitivity level "top secret" must have been identification that is certified by SKIP (Simple Key Management for Internet Protocols) and if the communication path does not have a "top secret" trust level, the session must be encrypted with the 3DES algorithm (column 19, lines 37-41).

In the present invention, by contrast, the term "specific character string" refers to a character string used in a document to be accessed, such that, if the document includes the specific character string, access to the document is limited to a permitted user or permitted users in accordance with the access level associated

with the specific character string (see application figures 2 and 3, and related discussion). There is nothing in Schneider to suggest that the "minimum encryption" and "minimum authentication" requirements are specified in the documents to be accessed. Rather, it is clear that they reside only in table of figure 6. Therefore, it is submitted that, contrary to the Examiner's assertions, the encryption and authentication requirements specified in figure 6 of Schneider do not correspond to the "specific character string" of the present invention.

The Examiner's arguments do not appear to address the limitation "wherein said identification data is added to said document if said document includes said specific character string," recited in claim 1. In Numao, access to documents in data file 210 (figure 2) is determined in access control subsystem 240 on the basis of a "policy description" 140 figure 3). As described in the Background Art section of Numao (see, for example, column 1, lines 17-27), the term "policy description" refers to one of a set of rules used to determine whether to permit access, the rules being arranged in a list of elements commonly called an access control list (ACL). In Numao, the ACL consists of a Subject (access permitted user), Object (target to be accessed), Operation (access permitted operation) and Condition (access permission condition) (see, for example, Figure 6 and description in col. 11, lines 35-42). Numao describes the policy descriptions 140 as residing in the resource document 40. Numao fails to teach or even suggest that a policy description, or any specific data included in a policy description, is added to a document to be accessed by a user, as claim 1 would require.

As noted by the Examiner, Schneider discloses that each of the access filters 203 has a copy of the access control database 301 that holds all data relevant for access control in the VPN (Virtual Private Network). However, Schneider, like Numao, fails to teach or suggest in any way, adding any form of identification data specifying access control information to the documents to be accessed.

Since the access control techniques for documents in Schneider are based on predetermined encryption and authentication requirements, and do not involve searching for a "specific character string" and adding associated identification data to documents having the character string, it is clear that Schneider also fails to

disclose the related limitation " access to said document is limited in accordance with contents of said access controlling information, when the access to said document is thereafter requested, if said document contains said added identification data." The text in Schneider referenced by the Examiner in this regard (column 19, lines 10-20), merely discusses the role of the network administrator in establishing appropriate encryption and authentication requirements corresponding to different trust/data sensitivity levels, and, therefore, does not appear to be relevant to the limitation in question.

In general, the invention in Schneider is directed to a security technology using a plurality of access filters, such as firewalls, to control access through the Internet by a roaming user to private networks or servers that form parts of a virtual private network (see, for example, Schneider figure 2). In Schneider, user access to the virtual private network is controlled in accordance with authentication and encryption requirements stored in an access control database resident in each access filter (column 8, lines 24-27, 30-34 and 60-63). On the other hand, the present invention is directed to an access control technology relating to individual documents stored on a server. In the present invention, user access to a document is in accordance with access controlling information associated with a specific character string, if the character string is present in the document. Thus, the teaching in Schneider is significantly different from that in the present invention or Numao, placing in serious doubt the Examiner's assertion that one of ordinary skill in the art would have been motivated to combine the teachings of the two references. The Applicants further believe that even if the references were combined, the combination would not result in the claimed invention.

For at least the foregoing reasons, it is respectfully submitted that claim 1 patentably distinguishes over the applied prior art references, whether considered individually or in combination. It is further submitted that claims 2-16 are allowable for at least the reason that they depend directly or indirectly, from claim 1.

The dependent claims also recite features that independently distinguish over the applied prior art. For example, claim 3, as well as claim 16, recites the

limitation "wherein it is defined whether or not said document includes said specific character string at one of a time when said document is registered, a time when said access controlling information is registered, and a time when the access to said document is requested." In the Action, the Examiner points to Numao figure 4, item 401, and column 9, line 61-65, as disclosing this feature. What the referenced figure and text discloses is that the policy evaluation module 10 detects, from the resource document 40, a policy description 140 that corresponds to the document that is to be accessed (step 401), and performs a evaluation of the extracted policy description 140 (step 402). However, there is no disclosure in Numao of any determination as to whether a specific character string is included or not in a document, or of any examination of a document "when said document is registered" or "when said access controlling information is registered."

Claims 6-8, 10 and 13 recite the limitation "wherein said access controlling information is provided in a single record comprising a plurality of fields, including ID information for identifying said record, and said ID information is added to the document for relating said access controlling information to the document." Regarding these claims, the Examiner points to Numao Figure 6 and asserts that the "ID information" corresponds to the object name or the target document to be accessed. However, the ID information is defined in claim 6 as "ID information for specifying said record" and is obviously different from the document name to be accessed. Unlike the scheme in Numao, the ID information in the present invention is associated with a set of "access controlling information" and not with any specific document, as many documents may include the same character string.

All of the Examiner's concerns having been addressed, it is respectfully submitted that the application is now in condition for allowance. Such action and the passing of this case to issue are respectfully requested.
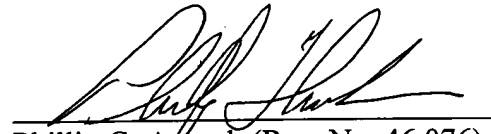
[Continued on next page]

Should the Examiner feel that a conference would help to expedite the prosecution of the application, the Examiner is hereby invited to contact the undersigned counsel to arrange for such an interview.

Respectfully submitted,

August 15, 2005
Date

Phillip G. Avruch (Reg. No. 46,076)
RABIN & BERDO, P.C.
(Customer No. 23995)
Telephone: (202) 371-8976
Telefax : (202) 408-0924
E-mail : firm@rabinchamp.com

PGA/